CLAIMS

What is claimed is:

1. A method for enabling encryption and decryption of an initial version of a software product comprising the steps of:

generating a first encryption key;

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;

generating a first key portion of said first encryption key;

calculating a second key portion by utilizing said first key portion and said first encryption key to generate a said second key portion such that the combination of said first key portion and second key portion form said first encryption key;

providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product;

combining said first key portion and said second key portion to provide said first encryption key in said hardware product; and

utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product.

2. The method of claim 1 wherein said step of generating a first encryption key utilizes a random number generator to generate said first encryption key.

3. The method of claim 1 wherein said step of calculating a second key portion utilizes an "exclusive or" logic operation to combine said first key portion and said first encryption key to calculate said second key portion.

4. The method of claim 1 wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation to combine said first key portion and said second key portion to provide said first encryption key.

5. The method of claim 1 further enabling an update of said first encryption key to provide a second encryption key to secure a different version of the initial software product, further comprising the steps of:

generating the second encryption key;

encrypting the different version of the initial software product with the second encryption key to provide an encrypted different version of the software product;

combining the first encryption key and the second encryption key to provide a third key portion;

installing said third key portion and the encrypted different version of the software product in said hardware product;

combining said third key portion and said second key portion to generate a fourth key portion in said hardware product;

combining the first key portion and the fourth key portion to provide said second encryption key in said hardware product; and

using the second encryption key to decrypt the encrypted different version of the software product.

6. The method of claim 5 wherein said step of providing said second encryption key utilizes a random number generator to generate said second encryption key.

7. The method of claim 5 wherein said step of combining the first encryption key and the second encryption key utilizes an "exclusive or" logic operation to combine said first encryption key and said second encryption key to generate said third key portion.

8. The method of claim 5 wherein said step of providing said second encryption key utilizes an "exclusive or" logic operation to combine said first key portion and said fourth key portion to provide said second encryption key.

9. The method of claim 5 wherein said initial version of software product and said different version of said initial version of said software product are non-sequential versions.

10. The method of claim 5 wherein said second encryption key is non-sequential with said first encryption key.

11. A method for providing for the security of encryption keys for encryption and decryption of an initial version of a software product provided by a provider to a user of a hardware product, said method comprising:

providing a first encryption key;

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;

providing a first key portion;

utilizing said first key portion and said first encryption key to calculate a second key portion such that the combination of said first and second key portions form said first encryption key;

storing said first key portion in storage means external to the hardware;

storing said second key portion separately from said first key portion in a tamper proof memory means in the hardware product;

storing said encrypted software product in a further memory means in the hardware product;

combining said first key portion and said second key portion in the hardware product to provide said first encryption key; and

decrypting said encrypted initial software product with said first encryption key.

12. The method of claim 11 wherein said step of providing a first encryption key utilizes a random number generator to generate said first encryption key.

13. The method of claim 11 wherein said step of utilizing said first key portion and said first encryption key to calculate said second key portion utilizes an "exclusive or" logic operation.

14. The method of claim 11 wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation performed by said hardware product.

15. The method of claim 11 further enabling security of an update of said first encryption key and providing a second encryption key for encrypting a different version of the initial software product, further comprising:

generating the second encryption key;

encrypting the different version of the initial software product with said second encryption key to provide an encrypted different version of the initial software product;

combining said first encryption key and said second encryption key to provide a third key portion;

installing said third key portion in said tamper proof memory means;

installing said encrypted different version of the initial software product in said further memory means in the hardware product;

combining said third key portion and said second key portion to generate a fourth key portion in the hardware product;

combining said first key portion and said fourth key portion to provide said second encryption key in the hardware product; and

using said second encryption key in the hardware product to decrypt the encrypted different version of the initial software product.

16. The method of claim 15 wherein said step of generating a second encryption key utilizes a random number generator.

17. The method of claim 15 wherein said step of combining said first encryption key and said second encryption key to generate a third key portion utilizes an "exclusive or" logic operation.

18. The method of claim 15 wherein said step of combining said first key portion and the fourth key portion to provide said second encryption key utilizes an "exclusive or" logic operation.

19. The method of claim 15 wherein said initial version of a software product is non-sequential with said different version of the initial software product.

20. The method of claim 15 wherein said second encryption key is non-sequential with said first encryption key.